



# Department of Homeland Security Daily Open Source Infrastructure Report for 13 November 2006

Current  
Nationwide  
Threat Level is

**ELEVATED**  
SIGNIFICANT RISK OF  
TERRORIST ATTACKS

[For info click here](http://www.dhs.gov/)

<http://www.dhs.gov/>

## Daily Highlights

- Federal Computer Week reports that the Nuclear Regulatory Commission has issued a final rule on reporting requirements for various transactions involving radioactive materials that will involve establishing secure, Web-based access to a new National Source Tracking System. (See item [1](#))
- The Associated Press reports that Department of Homeland Security Secretary Michael Chertoff marked Veterans Day by helping christen U.S. Coast Guard Cutter Bertholf, the first of a new class of ships called National Security Cutters. (See item [12](#))

### DHS Daily Open Source Infrastructure Report Fast Jump

Production Industries: [Energy](#); [Chemical Industry and Hazardous Materials](#); [Defense Industrial Base](#)

Service Industries: [Banking and Finance](#); [Transportation and Border Security](#); [Postal and Shipping](#)

Sustenance and Health: [Agriculture](#); [Food](#); [Water](#); [Public Health](#)

Federal and State: [Government](#); [Emergency Services](#)

IT and Cyber: [Information Technology and Telecommunications](#); [Internet Alert Dashboard](#)

Other: [Commercial Facilities/Real Estate, Monument & Icons](#); [General](#); [DHS Daily Report Contact Information](#)

## Energy Sector

**Current Electricity Sector Threat Alert Levels: Physical: Elevated, Cyber: Elevated**

Scale: LOW, GUARDED, ELEVATED, HIGH, SEVERE [Source: ISAC for the Electricity Sector (ES-ISAC) –

<http://www.esisac.com>]

1. *November 08, Federal Computer Week* — **NRC rule creates Web system to track nuclear material.** The Nuclear Regulatory Commission (NRC) has issued a final rule on reporting requirements for various transactions involving radioactive materials that will involve establishing secure, Web-based access to a new National Source Tracking System (NSTS). States and the NRC will use NSTS to closely track the location and use of various radioactive materials. Although those materials are used in a range of applications in industries such as oil and gas, construction, food, and medicine, and a number of separate systems contain information on companies and individuals who are licensed to use them, no one system covers

all licensees. In a report earlier this year, however, the NRC's inspector general warned that the Web-based system may be inadequate because the supporting regulatory analysis, which provides the framework for the system, is based on unreliable data from an interim database. That interim database of "sources of concern" was created several years ago, although reporting to it is voluntary. NSTS will be mandatory, and all licensed handlers of materials governed by the new rule will have to report their inventories and transactions by the end of November 2007.

Source: <http://www.fcw.com/article96756-11-08-06-Web>

2. *November 07, Reuters* — **China doubling coal mine shutdowns.** The northern Chinese province of Shanxi, where 19 miners died in a gas blast on Sunday, November 5, will close more coal mines by mid-2008 to raise safety conditions and better protect the environment, Xinhua news agency said. The government could increase to 1,100 the number of coal mines to be shut by June 2008, up from an originally listed 500, Xinhua said. Coal produced in Shanxi, where there are about 3,500 collieries, accounts for a third of the country's output, it said. In the year to June, the province closed more than 1,000 coal mines, Xinhua added. China is struggling to meet booming demand for coal, which fuels about 70 percent of its energy consumption. In the rush for profits, safety regulations are often ignored, production is pushed beyond limits and dangerous mines that have been shut down are reopened illegally. Around 3,630 miners died in over 2,000 accidents in the first 10 months of the year, although the grim total represents some improvement on 2005, when the industry claimed nearly 6,000 lives.

Source: [http://www.cnn.com/2006/WORLD/asiapcf/11/07/china.coal.reut/index.html?section=cnn\\_latest](http://www.cnn.com/2006/WORLD/asiapcf/11/07/china.coal.reut/index.html?section=cnn_latest)

[\[Return to top\]](#)

## **Chemical Industry and Hazardous Materials Sector**

Nothing to report.

[\[Return to top\]](#)

## **Defense Industrial Base Sector**

3. *November 08, Government Accountability Office* — **GAO-07-226CG: DoD Transformation: Challenges and Opportunities (Presentation by the Comptroller General).** The Honorable David M. Walker, Comptroller General of the United States, delivered a presentation before the Defense Acquisition University's Program Executive Officers/Systems Command Commanders conference in Fort Belvoir, VA. In the presentation, he discusses systemic defense acquisition challenges. Some of the key challenges include: 1) Service budgets are allocated largely according to top line historical percentages rather than Defense-wide strategic assessments and current and likely resource limitations; 2) Capabilities and requirements are based primarily on individual service wants versus collective Defense needs that are both affordable and sustainable over time; 3) Defense consistently over-promises and under-delivers in connection with major weapons, information, and other systems; 4) Defense often employs a "plug and pray approach" when costs escalate. To view the full presentation, please see the source.

Source: <http://www.gao.gov/cghome/d07226cg.pdf>

## **Banking and Finance Sector**

4. *November 09, IDG News Service* — **Consumers to lose \$2.8B to phishers in 2006; Gartner says fewer, but bigger, attacks will gain more for criminals.** Browser makers may have added new antiphishing features to their products in recent months, but the criminals are still gaining ground in their efforts to defraud U.S. consumers, according Gartner. Phishers have hit more victims with their online attacks, and while fewer people are losing money to phishers, successful attempts have been yielding bigger payoffs, said Avivah Litan of Gartner. "When they do succeed, they're stealing five times more than they stole last year." The average loss per phishing attack was \$1,244 this year, Litan said, up from \$256. Gartner estimates that the total financial losses attributable to phishing will total \$2.8 billion this year. And users who are taken in by phishing scams are less likely to recover their money, Litan said. In 2005, 80 percent of victims got their money back. This year, that number dropped to 54 percent. Gartner estimates that 3.5 million Americans will give up sensitive information to phishers in 2006 — up from an estimated 1.9 million last year. Although the recently released Internet Explorer 7 and Firefox 2.0 browsers came with new antiphishing features, Microsoft, and Mozilla are still playing catch-up with the crooks.

Source: [http://www.infoworld.com/article/06/11/09/HNgartnerphishing\\_1.html](http://www.infoworld.com/article/06/11/09/HNgartnerphishing_1.html)

5. *November 09, Websense Security Labs* — **Multiple Phishing Alert: Crane Federal Credit Union, HawaiiUSA Federal Credit Union, Northern Federal Credit Union, Arizona Bank & Trust, Ouachita Independent Bank.** Websense Security Labs has received new reports of phishing attacks. In all of the attacks, an e-mail provides a link to a phishing site that attempts to collect personal and account information.

Crane Federal Credit Union: A spoofed e-mail message claims that if users take part in a survey, \$100 will be credited to their account.

HawaiiUSA Federal Credit Union: A spoofed e-mail message claims that in order to receive an important announcement, users will have to confirm their e-mail address online.

Northern Federal Credit Union: A spoofed e-mail message claims that if the services listed are not going to be renewed immediately, they will be suspended.

Arizona Bank & Trust: A spoofed e-mail message claims that, due to a periodic review of customer accounts, users will have to log on to verify their online information.

Ouachita Independent Bank: A spoofed e-mail message claims that in order to get important announcements from the bank users must verify their e-mail address.

Screenshots:

<http://www.websensesecuritylabs.com/alerts/alert.php?AlertID=696>

<http://www.websensesecuritylabs.com/alerts/alert.php?AlertID=694>

<http://www.websensesecuritylabs.com/alerts/alert.php?AlertID=693>

<http://www.websensesecuritylabs.com/alerts/alert.php?AlertID=690>

<http://www.websensesecuritylabs.com/alerts/alert.php?AlertID=691>

Source: <http://www.websensesecuritylabs.com/>

6. *November 08, This Day (Africa)* — **Cybercrime group warns banks against hackers.** Coordinator of the Nigerian Cybercrime Working Group, Basil Udotai, has disclosed that the

consolidation of banks has made them vulnerable to on-line crimes. Udotai said the increase in the capital base of banks had enlisted them among the big financial houses in the world, making targets of high level on-line hackers. Udotai said the hackers invest a lot of money to buy communication equipment for high level crimes and only big banks attract their interest. Aome of the banks had already brought complaints of Website cloning by unknown persons and the risks would keep increasing as their investments continue to grow. He stressed the need for all banks to build a "virtual center" where they would be sharing information from time to time instead of hoarding facts for fear of competition. The center for sharing information must be based on a framework of "readiness, responsiveness, and resilience "and the benchmarking of global best practices in checking hackers. Access banks, UBA, Diamond bank, and Skye bank agreed to endorse a synergy known as FinCERT Nigeria project to take pro-active measures against hackers.

Source: <http://www.thisdayonline.com/nview.php?id=62683>

7. *November 08, News Observer (NC)* — **D.C. man convicted in ID theft ring.** A federal jury in Raleigh, NC, convicted a former security guard for his role in using stolen identities of federal employees to open bogus retail accounts and purchase cell phones, authorities announced this week. Xavier Vidal Jennette of Washington, D.C. was convicted of conspiracy, wire fraud, and aggravated identity theft. Anthony Durand Wallace, Aiesha Demetria Horton, and Toya Lenette Sadler all conspired with Jennette in what the U.S. Attorney's Office described as an "extensive identity theft ring" in the Raleigh, NC, area. The criminal enterprise started in Virginia where the names and Social Security numbers of more than 40 employees were stolen and used at retail outlets. Jennette worked as a facilities security officer for a government contractor in Alexandria, VA. He had top secret security clearance and was entrusted with the personal information of more than 120 employees. Jennette stole the employees' personal information when he ended his employment with the contractor in 2004 and brought the information to North Carolina. Wake authorities were tipped off about the scam when one of the victims noticed a mistake on a financial account and reported it to police.

Source: <http://www.newsobserver.com/102/story/507743.html>

8. *November 07, Government Computer News* — **Analytics capture mortgage fraud trends.** The Financial Crimes Enforcement Network (FinCEN) found through an analysis of suspicious-activity reports that suspected mortgage loan fraud rose 35 percent in the past year. FinCEN, an agency of the Treasury Department, began an assessment of suspected mortgage loan fraud after noticing in its routine analysis a spike in suspicious-activity reports (SARs) containing certain characteristics of suspicious activity, a FinCEN spokesperson said. FinCEN uses analytics software to examine the reports of suspicious bank and financial-institution transactions under the Bank Secrecy Act. Individually or over time, these transactions could indicate money laundering, terrorist financing, fraud, and other financial crimes. Many of the SARs reviewed included more than one characterization of suspicious activity in addition to mortgage fraud. "False statement" was the most reported activity in conjunction with mortgage loan fraud, while "identity theft" was the fastest-growing secondary characterization reported.

Source: [http://www.gcn.com/online/vol1\\_no1/42547-1.html?topic=busine](http://www.gcn.com/online/vol1_no1/42547-1.html?topic=busine)  
ss\_process\_management

[[Return to top](#)]

## **Transportation and Border Security Sector**

9. *November 11, Associated Press* — **Rail crew tried brakes before derailment.** Crew members aboard a runaway maintenance train that barreled down a steep Sierra Nevada slope tried frantically to slam on the emergency brakes before the locomotive derailed, investigators said. The bodies of two crew members were recovered Friday, November 10, from the smoldering wreckage of Thursday's derailment, which spilled thousands of gallons of fuel near a thick forest and sparked a large fire. Eight other crew members aboard the train, which was carrying rail equipment, suffered minor injuries. Survivors told authorities that the men who died had been trying to apply the brakes when the train ran off the tracks in a ravine about 60 miles east of Sacramento. The emergency brakes slowed the locomotive only slightly before the train's supervisor — in a final, desperate move — threw it into reverse, said Dave Watson, lead investigator for the National Transportation Safety Board. The train kept rolling and gathering speed, eventually hitting a curve at about 50 mph — twice the recommended speed for that stretch of tracks. Investigators have come close to ruling out the possibility of faulty tracks at the crash site and are focusing instead on the speed of the train.

Source: <http://timesunion.com/AspStories/story.asp?storyID=533476&category=&BCCode=&newsdate=11/11/2006>

10. *November 11, Associated Press* — **Damage on Chicago train line prompts passenger evacuation.** About 100 passengers were evacuated Friday, November 10, from trains stuck in a subway after track damage caused the power to be cut. Six people were taken to hospitals with minor injuries. Service on the Red Line's underground portion was suspended for almost three hours while the passengers were safely evacuated and Chicago Transit Authority (CTA) workers investigated the problem, said CTA spokesperson Sheila Gregory. It was the second incident involving CTA trains in less than six months. One of the CTA's Blue Line trains — which travel to O'Hare International Airport — derailed in July. That incident sparked a smoky fire, and about 150 people were hospitalized, mostly for smoke inhalation. In Friday's incident, Gregory said a loose part of a train damaged a portion of the track's electrified third rail at about 10 a.m. near the North/Clybourn stop on the Red Line, which runs between the city's North and South Sides. Power was cut to the subway system, stranding a total of eight trains, Gregory said.

Source: [http://www.mercurynews.com/mld/mercurynews/news/breaking\\_news/15981670.htm](http://www.mercurynews.com/mld/mercurynews/news/breaking_news/15981670.htm)

11. *November 11, Los Angeles Times* — **Report of armed man closes John Wayne Airport.** Orange County's John Wayne Airport was shut down and hundreds of passengers were delayed for more than an hour Friday, November 10, as airport officials investigated a report that a boarding passenger had pulled a weapon out of a duffel bag. Lt. Lloyd Downing, a spokesperson for the Orange County Sheriff's Department, said "It was a security breach and the [Transportation Security Administration] ordered a complete shutdown." The unidentified passenger was detained but no weapon was found, Downing said. The incident began about 6 p.m., PST he said, when someone reported seeing the man pull a weapon in Terminal B. Authorities did not say what type of weapon it was. As officers questioned him, the airport's two terminals were searched. In the meantime, airport spokesperson Jenny Wedge said, nine planes that had landed waited with passengers aboard while all outgoing flights were delayed. At least two flights were canceled.

Source: <http://www.latimes.com/news/printedition/california/la-me-ai>



12. *November 11, Associated Press* — **Cutter damaged in Katrina is christened.** The first large U.S. Coast Guard cutter to be built in 35 years was christened Saturday, November 11, more than a year after Hurricane Katrina damaged it in the shipyard during construction. Department of Homeland Security Secretary Michael Chertoff marked Veterans Day by helping christen the 418-foot, 4,300-ton Bertholf, which the Coast Guard calls a "national security cutter." It is about a third larger than the class of ships it replaces. The Coast Guard ordered the Bertholf and seven other deep-water cutters as part of a multibillion-dollar program to replace an aging fleet. Rescue operations aren't the only use for the new high-endurance ships — they will also play critical roles in fighting terrorism, drug smuggling and illegal immigration. The Bertholf, which is scheduled to be commissioned in early 2008, has vastly superior communications and weapons systems, a larger flight deck and more comfortable living quarters than its predecessors, the Coast Guard said.

Additional information about USCGC BERTHOLF:

<http://www.uscg.mil/deepwater/gallery/nscgallery.htm>

Source: <http://www.chron.com/dispatch/story.mpl/ap/nation/4327855.html>

13. *November 09, Bay City News (CA)* — **SFO pilot cargo screening program to expand.** A \$30 million air cargo-screening pilot program that began operation at San Francisco International Airport in June is set to expand to Seattle's Seattle-Tacoma International Airport, according to the U.S. Department of Homeland Security (DHS). The Air Cargo Explosives Detection Pilot Program was designed to help officials better understand the technological and operational issues associated with detecting explosives or people that might be hidden in cargo. The program uses existing cargo screening technologies, but scientists have also worked on developing new screening devices, including advanced X-ray systems. The program uses powerful machines that have detection capabilities comparable to computed tomography scan devices. When the program is implemented in Seattle, tests will focus on assessing the flow of air cargo and the pace at which it must be screened. Tests will also address detecting carbon dioxide, which may indicate the presence of a person in cargo, according to DHS. Research is also under way to develop new detection systems such as an X-ray that can scan entire pallets at a time to detect explosives, according to the department.

Source: <http://abclocal.go.com/kgo/story?section=local&id=4746656>

[[Return to top](#)]

## **Postal and Shipping Sector**

14. *November 09, Virginian-Pilot* — **Flames at Virginia post office sicken 39 workers, delay mail.** A dangerously high level of carbon monoxide at the downtown post office in Suffolk, VA, sent 39 employees to the hospital Wednesday morning, November 8, and caused widespread delays in mail service to homes. No one was seriously hurt from the fumes, officials said. The post office aimed to complete its 28 delivery routes by Wednesday night after all its employees returned from the hospital, said Gene Bunn, manager of Post Office Operations for the Tidewater Area. Two generators running outdoors on a loading dock caused the carbon monoxide problem.

Source: <http://content.hamptonroads.com/story.cfm?story=114046&ran=4.5152>

15. *November 08, Winnipeg Sun (Canada)* — **International shipping containers are 'Trojan horses' for terrorists, drug smugglers.** The thousands of international shipping containers landing on North American shores each day are "Trojan horses" for terrorists and drug smugglers, a major port operator is warning. "It is a question of time, in my opinion, that a container will be delivering either a dirty bomb or the goods to help terrorists," Greg Gilbert, senior vice-president for Hutchison Port Holdings. "Many people say the best delivery system for a dirty bomb might be a truck or a small boat, but to get it across the ocean it has to be in a container." Gilbert's comments came last week in a submission to the Senate committee on national security and defense. He urged governments to regulate tougher inspections that would include X-rays, radiation screening and checks for container tampering in order to ensure weapons aren't being taken to a Canadian or U.S. port.

Source: <http://winnipeg.sun.com/News/Canada/2006/11/08/2276663-sun.html>

16. *November 08, DM News* — **UPS to offer three daily time-definite delivery options.** In the largest expansion of its international shipping portfolio in more than a decade, United Parcel Service (UPS) said it would begin offering customers three, rather than two, daily time-definite delivery options to and from the world's most active trading markets. The changes, which take effect on January 1, expand the number of morning and afternoon commit times UPS offers for urgent deliveries to and from cities throughout the world. In addition to expanded end-of-day options, Atlanta-based UPS now will offer 9 a.m. delivery guarantees from U.S. origins to more cities in Asia and other global destinations than any other carrier.

Source: <http://www.dmnews.com/cms/dm-news/direct-mail/38904.html>

17. *November 08, News Journal (DE)* — **Three teens charged in mailbox explosion.** Three teenagers have been arrested in connection with an acid bomb explosion inside a mailbox in Middletown, DE. Chief Deputy Fire Marshal Alan Brown said more arrests are expected in the October 7 incident that resulted in nearly \$1,500 in property damage.

Source: <http://www.delawareonline.com/apps/pbcs.dll/article?AID=/20061108/NEWS/61108059>

18. *November 06, KFMB (CA)* — **Homemade bomb blows up in California mailbox.** Sheriff's investigators are thankful a mailbox bomb did not cause as much as it could have in Lakeside, CA, on Monday, November 6. Neighbors were frightened, but no one was hurt when the homemade device went off inside of a mailbox on Melrose Lane near Sunglow Drive. "Basically it didn't blow up the mailbox, but if a person walked up to it and opened up the mailbox and if it was going to function, it could have killed somebody. But like I say, it did not function the way it's supposed to as an [improvised explosive device]," Sgt. Conrad Grayson said.

Source: <http://www.kfmb.com/stories/story.69256.html>

[[Return to top](#)]

## **Agriculture Sector**

19. *November 09, Rocky Mountain News (CO)* — **Two bull moose test positive for chronic**

**wasting disease.** Two bull moose that hunters took legally southeast of Glendevy, CO, about 25 miles west of Red Feather Lakes in the Rawah Wilderness, tested positive for chronic wasting disease (CWD). The moose were from game management units 6 and 7. The Colorado Division of Wildlife said both moose were killed in October and their heads were submitted for testing. CWD is a fatal neurological disease that has been diagnosed in wild deer and elk in ten states and two Canadian provinces. It attacks the brains of animals and is always fatal. It isn't known if the disease can be transmitted to humans who eat the animal but as a precaution, hunters are advised not to eat meat from diseased animals.

Source: [http://www.rockymountainnews.com/drmn/local/article/0.1299.DRMN\\_15\\_5131108.00.html](http://www.rockymountainnews.com/drmn/local/article/0.1299.DRMN_15_5131108.00.html)

[\[Return to top\]](#)

## **Food Sector**

Nothing to report.

[\[Return to top\]](#)

## **Water Sector**

**20. *November 09, Palm Beach Post* — Water limits planned in South Florida because of drought.** South Florida has entered its first drought in five years, prompting water managers to plan mandatory restrictions for farms, businesses and residents around Lake Okeechobee starting November 17. The cuts will affect everyone who draws water directly from Lake Okeechobee, the St. Lucie Canal and the Caloosahatchee River. Those cuts will primarily hit growers, who say they lost \$100 million during the region's last drought in 2000 and 2001, and are aimed at reducing that area's water use by 15 percent. Residents in the affected area, including Pahokee, Belle Glade, South Bay and other Glades cities, will face limits of three days a week watering lawns and landscaping. The board also will consider issuing a warning urging residents and businesses to conserve in Palm Beach, Broward, Miami-Dade and Monroe counties. But water managers said they plan no mandatory cuts for that region's 4 million residents.

Source: [http://www.palmbeachpost.com/localnews/content/local\\_news/epaper/2006/11/09/m1b\\_Water\\_1109.html](http://www.palmbeachpost.com/localnews/content/local_news/epaper/2006/11/09/m1b_Water_1109.html)

[\[Return to top\]](#)

## **Public Health Sector**

**21. *November 09, Associated Press* — Eleven million bottles of acetaminophen recalled.** A major manufacturer of store-brand acetaminophen recalled 11 million bottles of the pain-relieving pills Thursday, November 8, after discovering some were contaminated with metal fragments. Perrigo Co. said it discovered the metal bits during quality-control checks. There were no immediate reports of injuries or illness. The recall affects bottles containing various amounts of 500-milligram caplets.

Source: <http://www.orlandosentinel.com/news/sns-ap-drug-warning.0.15>



22. *November 08, News—Medical (Australia)* — **Global resurgence in zoonotic viral diseases.** Doctors and veterinarians need to work together to tackle the increasing global threat of zoonotic viral diseases spread by non-human vertebrate hosts — including dogs, cattle, chickens and mosquitoes — according to a review in the November issue of *Journal of Internal Medicine*. An estimated 50 million people acquired zoonotic diseases between 2000 and 2005 and up to 78,000 have died, reports Dr. Jonathan Heeney, Chair of the Department of Virology at the Biomedical Primate Research Center in the Netherlands. And the diseases responsible for the majority of zoonotic illnesses, and a third of the deaths in the study period, appear to be increasing. This is particularly worrying because there are no effective vaccines for some of the most common zoonotic viruses. "Viral infections with zoonotic potential can become serious killers once they are able to establish the necessary adaptations for efficient human-to-human transmission under conditions sufficient to reach epidemic proportions" says Dr. Heeney. "That is why it is so important for experts from all walks of medicine to work more closely together." Abstract: <http://www.blackwell-synergy.com/doi/abs/10.1111/j.1365-2796.2006.01711.x> Source: <http://www.news-medical.net/?id=20932>
23. *November 08, Canadian Broadcasting Corporation* — **Quebec orders coroner's inquest into C. difficile deaths.** A coroner's inquest will investigate a C. difficile outbreak that left 11 patients dead at a Quebec, Canada, hospital, the government announced Wednesday, November 8. There is sufficient evidence to suggest minimum sanitation standards were not enforced at the Centre hospitalier Honoré-Mercier in Saint-Hyacinthe, where a flare-up of the clostridium difficile bacteria infected dozens of elderly patients over the summer, said Quebec Health Minister Philippe Couillard. Source: <http://www.cbc.ca/canada/montreal/story/2006/11/08/cdifficile-coronersinquest.html>
24. *November 08, Ashley County Ledger (AR)* — **Chicken pox cases in Arkansas county now at 176.** Ashley County, AR, has had a total of 176 cases of chicken pox since the outbreak began in early September, Ann Wright of the Arkansas Department of Health said Tuesday, November 7. Wright said, "What is unusual is that we are seeing cases in people that have had two doses of vaccine." She noted that representatives of the Centers for Disease Control and Prevention were in Hamburg two weeks ago to gather information on the outbreak, but said that as of Tuesday, the state health department has not received their report on the outbreak. The initial outbreak was in elementary age children, but the disease is now affecting all ages, she said. Source: [http://www.ashleycountyledger.com/articles/2006/11/08/news/h\\_16f103g.txt](http://www.ashleycountyledger.com/articles/2006/11/08/news/h_16f103g.txt)
25. *November 07, Atlanta Journal—Constitution* — **CDC will not release Hurricane Katrina response report.** The Centers for Disease Control and Prevention (CDC) has critiqued its response to Hurricane Katrina and says it's taking actions to ensure that the agency is better prepared in the future. But the Atlanta-based CDC is keeping secret the report analyzing its performance, and is talking only generally about the problems it identified, saying they are being addressed with better plans, communication and training. The CDC dispatched 700 staffers to help prevent disease and care for those who were displaced, and has received praise from local officials for playing a critical role in vaccinating residents and monitoring for disease outbreaks. But behind the scenes, the CDC ran into problems commanding and

controlling its response, the agency acknowledged in a document posted on its Website. While the CDC was in charge of only a small portion of the federal response to Katrina, its performance is, in the agency's words, a "gauge" of its ability to coordinate logistics in a major public health crisis. CDC officials said they are taking a wide range of actions as a result of lessons learned from Katrina to better prepare the agency for a crisis, such as a flu pandemic. CDC's lessons learned from Katrina: [http://www.cdc.gov/about/news/2006\\_11/katrina.htm](http://www.cdc.gov/about/news/2006_11/katrina.htm)  
Source: [http://www.ajc.com/news/content/news/stories/2006/11/07/1107\\_cdckatrina.html](http://www.ajc.com/news/content/news/stories/2006/11/07/1107_cdckatrina.html)

26. *November 01, Journal of Emerging Infectious Diseases* — **Study: Food markets with live birds as a source of avian influenza.** A patient may have been infected with highly pathogenic avian influenza virus H5N1 in Guangzhou, People's Republic of China, at a food market that had live birds. Virus genes were detected in 1 of 79 wire cages for birds at nine markets. One of 110 persons in the poultry business at markets had neutralizing antibody against H5N1. A study recently published in the Journal of Emerging Infectious Diseases examines food markets with live birds as a source of avian influenza. Refer to the source to view the full study.  
Source: <http://www.cdc.gov/ncidod/EID/vol12no11/06-0675.htm>

[[Return to top](#)]

## **Government Sector**

27. *November 09, Associated Press* — **Buses on school trip collide; 15 students injured.** Three charter buses collided early Thursday, November 9, after the brakes on one apparently failed, injuring at least 15 middle school students on a field trip to the Atlantic coast, officials said. The students were in a caravan of six buses headed for Myrtle Beach, SC, when three of the buses crashed in Erwin, between Raleigh and Fayetteville. Two of the buses had stopped at a traffic light at U.S. 421 when the last bus slammed into them. There were 143 students on the three buses. Most of those taken to Betsy Johnson Regional Hospital had cuts and bruises.  
Source: <http://www.cnn.com/2006/US/11/09/buses.colldie.ap/index.html>

28. *November 08, Associated Press* — **Two accused of death plot at Texas school.** Two high school students have been charged with conspiracy to commit murder after authorities uncovered what they described as a plot for a potentially deadly school attack. The boys, whose names were not released, were arrested Thursday, November 9, Williamson County, TX, Sheriff's Department Detective John Foster said. McNeil High has about 2,700 students and 200 staff members. Round Rock is about 15 miles north of Austin and is the headquarters of computer maker Dell Inc.  
Source: <http://www.azcentral.com/news/articles/1108schoolplot1108.htm>

[[Return to top](#)]

## **Emergency Services Sector**

29. *November 13, KCAL-TV (CA)* — **Los Angeles officials prepare for simultaneous disasters.** In California, officials practiced their response to a simulated earthquake and terrorist attack in Los Angeles County on Thursday, November 9, during "Operation Doubleheader." The Los

Angeles County Office of Emergency Management organized the 12-hour exercise to determine what information and help the public would need if a natural disaster and terrorist attack struck on the same day. In the scenario played out at the county's Emergency Operations Center east of downtown Los Angeles, a magnitude-6.5 earthquake occurs on the Verdugo fault with an epicenter near Bob Hope Airport in Burbank, followed by a series of explosions over a two-hour period that impact critical facilities in Los Angeles County.

Source: [http://cbs2.com/topstories/local\\_story\\_313160855.html](http://cbs2.com/topstories/local_story_313160855.html)

30. *November 10, Daily Bulletin (CA)* — **California first responders put to test in statewide disaster drill.** Local, state and federal agencies' preparedness for multiple disasters will undergo scrutiny in California next week when a three-stage, statewide drill begins Tuesday, November 14, in Devore with a mock "weapons of mass destruction" terror attack. The terror drill will be followed by an "outbreak" of avian flu in the Fresno area and an "earthquake" in the San Francisco Bay area, officials said. The statewide scenario concludes Thursday, November 16. The Hyundai Pavilion will be ground zero for the first part of the mock catastrophes, which will include a total of 1,500 participants from 105 local, state and federal agencies, San Bernardino County officials said. More than 1,000 first responders and 70 agencies will participate in the mock disaster at the Hyundai Pavilion.

Source: [http://www.dailybulletin.com/news/ci\\_4633157](http://www.dailybulletin.com/news/ci_4633157)

31. *November 10, Independent Record (MT)* — **First phase of emergency radio system complete in Montana.** Lewis and Clark County, MT, has completed the initial phase of a multimillion-dollar project to improve communications among a host of local, state, and federal agencies. The improvements unite emergency responders over a digital network that stretches beyond county lines to Deer Lodge, Fort Benton and the Bozeman area. It's the first such project in Montana. Another project stretching across the Canadian border is set to come online in the next year or so, and the network will eventually include the entire state. The new system allows seamless digital communications over about 95 percent of the county and enables peace officers, firefighters, ambulance personnel, and Public Works Department officials to talk to each other. The old analog system covered about 50 percent of the county and didn't allow for communications between the agencies. The radios function much like a cellular phone system, with units bouncing signals off towers, repeater stations, and microwave links across the county's mountains and valleys. The system will continue to broadcast analog signals along with the digital channels. Citizens with scanners will be able to hear most of the communications, but responders have the option of switching to an encrypted channel if need be.

Source: [http://www.helenair.com/articles/2006/11/10/helena/a09111006\\_01.txt](http://www.helenair.com/articles/2006/11/10/helena/a09111006_01.txt)

[\[Return to top\]](#)

## **Information Technology and Telecommunications Sector**

32. *November 08, Age (Australia)* — **SpamThru and Warezo responsible for rise in spam: MessageLabs report.** The number of e-mail viruses targeting Australians is on the rise, with Australia last month experiencing the biggest growth in attacks of any country. One in 84.1 e-mails or 1.2 percent of e-mail traffic contains a virus, up from 0.4 percent of e-mail traffic the month before, MessageLabs' Intelligence Report for October 2006 said. The global ratio

was 1 percent of e-mail traffic. This ranks Australia 12th out of all countries, where it was "previously at the bottom of the list," the report said. India remains the hardest hit country, with one in 16 e-mails containing a virus. It was followed by Ireland, Germany, Singapore and Spain. Responsible for much of the rise in viruses is a spam-sending Trojan dubbed "SpamThru," which MessageLabs said had increased global spam levels to almost three out of every four e-mails. The developers of SpamThru have so far managed to avoid detection by traditional anti-virus software, by releasing new strains of the Trojan at regular intervals, MessageLabs said. Another virus, Warezov, is also identified by MessageLabs as a contributing factor to the increase in spam. Like SpamThru, it hijacks the computers of unsuspecting users and turns them into spam distributors.

MessageLabs report: [http://www.messagelabs.com/publishedcontent/publish/threat\\_watch\\_dotcom\\_en/intelligence\\_reports/october\\_2006/DA\\_173834.html](http://www.messagelabs.com/publishedcontent/publish/threat_watch_dotcom_en/intelligence_reports/october_2006/DA_173834.html)

Source: <http://www.theage.com.au/articles/2006/11/08/1162661735244.html>

**33. *November 08, Security Focus* — Microsoft Excel file rebuilding remote code execution vulnerability.**

Microsoft Excel is prone to a remote code execution vulnerability. Successfully exploiting this issue allows attackers to corrupt process memory and to execute arbitrary code in the context of targeted users. Note that Microsoft Office applications include functionality to embed Office files as objects contained in other Office files. As an example, Microsoft Word files may contain embedded malicious Microsoft Excel files, making Word documents another possible attack vector.

For a complete list of vulnerable products: <http://www.securityfocus.com/bid/18938/info>

Solution: Microsoft has released a security advisory addressing this issue. For more information: <http://www.securityfocus.com/bid/18938/references>

Source: <http://www.securityfocus.com/bid/18938/discuss>

**34. *November 08, Security Focus* — Symantec Automated Support Assistant ActiveX control buffer overflow vulnerability.**

An ActiveX control shipped with Symantec Automated Support Assistant and some other Symantec products is prone to a stack-based buffer overflow vulnerability. This vulnerability requires a certain amount of user-interaction for an attack to occur, such as visiting a malicious Website. A successful exploit would let a remote attacker execute code with the privileges of the currently logged-in user. These products are shipped with the affected ActiveX control: Symantec Automated Support Assistant; Symantec Norton AntiVirus; Symantec Norton Internet Security; Symantec Norton System Works. Note that the Symantec Automated Support Assistant is used by support to identify problems running any Symantec consumer-based products. Therefore, the affected control may be present on computers running other consumer products and versions as well. Symantec Corporate and Enterprise products are not affected, because they do not install the affected control.

For a complete list of vulnerable products: <http://www.securityfocus.com/bid/20348/info>

Solution: Symantec has released fixes to address this issue. Fixes can be automatically applied through Symantec LiveUpdate. Users who may have downloaded or installed the Symantec Automated Support Assistant should visit the following location to obtain a fixed version:

<https://www-secure.symantec.com/techsupp/asa/install>.

A tool to remove vulnerable versions of the ActiveX control is available from the following location: [http://www.symantec.com/home\\_homeoffice/security\\_response/removealtools.jsp](http://www.symantec.com/home_homeoffice/security_response/removealtools.jsp)

Source: <http://www.securityfocus.com/bid/20348/references>

35. *November 08, Security Focus* — **IBM Websphere Application Server multiple vulnerabilities.** IBM Websphere Application Server is prone to multiple vulnerabilities. These issues include vulnerabilities of unknown impact, information disclosure vulnerabilities, and security bypass vulnerabilities. Other potentially security-related issues were also addressed. For a complete list of vulnerable products: <http://www.securityfocus.com/bid/17919/info>  
Solution: The vendor has released updated versions to address these issues. Contact the vendor for details on obtaining the appropriate updates.  
Source: <http://www.securityfocus.com/bid/17919/references>
36. *November 08, CNET News* — **Google accidentally sends out e-mail worm.** Google on Tuesday, November 7, inadvertently sent the Kama Sutra e-mail worm to the 50,000 subscribers of a Google Video e-mail group. Three messages were posted Tuesday evening to an e-mail list that sends out alerts about additions to the Google Video blog. "Some of these posts may have contained a virus called W32/Kapser.A@mm — a mass-mailing worm," Google said in a note on its Website apologizing for the incident. W32/Kapser.A is better known as the Kama Sutra worm. Some antivirus companies raised an alarm about the threat in February, but it ultimately shriveled.  
Source: [http://news.com.com/Google+accidentally+sends+out+e-mail+worm/2100-7349\\_3-6133829.html](http://news.com.com/Google+accidentally+sends+out+e-mail+worm/2100-7349_3-6133829.html)

### Internet Alert Dashboard

Current Port Attacks	
<b>Top 10 Target Ports</b>	15281 (---), 1026 (win-rpc), 4662 (eDonkey2000), 6881 (bittorrent), 1027 (icq), 4672 (eMule), 25530 (---), 1028 (---), 51586 (---), 445 (microsoft-ds) Source: <a href="http://isc.incidents.org/top10.html">http://isc.incidents.org/top10.html</a> ; Internet Storm Center
To report cyber infrastructure incidents or to request information, please contact US-CERT at <a href="mailto:soc@us-cert.gov">soc@us-cert.gov</a> or visit their Website: <a href="http://www.us-cert.gov">www.us-cert.gov</a> .	
Information on IT information sharing and analysis can be found at the IT ISAC (Information Sharing and Analysis Center) Website: <a href="https://www.it-isac.org/">https://www.it-isac.org/</a> .	

[[Return to top](#)]

## Commercial Facilities/Real Estate, Monument & Icons Sector

37. *November 11, Associated Press* — **Bomb blast at A&W restaurant in Jakarta mall.** A bomb exploded at an American fast food restaurant in the Indonesian capital on Saturday, November 11, seriously wounding a man believed to have been carrying the device. Al-Qaida-linked militants have carried out several bombings in the country in recent years, but police declined to speculate on the motive behind this blast, which comes less than two weeks before President Bush is due to visit on November 20. The low-explosive device shattered windows and broke chairs at the A&W restaurant in a shopping mall rarely visited by foreigners, police spokesperson Col. Ketut Untung Yoga said. An employee said that staff saw a man outside the restaurant who looked seriously ill and brought him inside to offer him help. A bomb then fell from his bag and detonated. The Islamic militant group Jemaah Islamiyah has been blamed for four attacks targeting Western interests in Indonesia since 2002, two in the capital and two on

the resort island of Bali that together killed more than 240 people.

Source: <http://www.cbsnews.com/stories/2006/11/11/ap/world/mainD8LAO HBG0.shtml>

- 38. *November 11, Trentonian (NJ)* — Bomb hoax disrupts neighborhood.** Police in Trenton, NJ, determined that a package in front of a home resembling a "bomb" was a hoax — an empty suitcase wrapped in brown tape and copper wire. Residents on Home Avenue between Beatty and Jersey streets were evacuated and the area closed to traffic, while a police bomb squad robot was used "to probe the briefcase and burst it open," according to Peter Page, Trenton Police spokesperson. Trenton Fire Department Capt. James Quinn said the suspicious package had been wrapped to appear like an explosive device, which was then detonated by the State Police. "It was a prank," he said. "There were no contents inside that would lead you to believe it was a real bomb. It was a hoax." "There's a lot of gang presence," one resident said. So far, nobody has claimed credit for the disruption.

Source: [http://www.zwire.com/site/news.cfm?newsid=17453183&BRD=1697&PAG=461&dept\\_id=44551&rft=6](http://www.zwire.com/site/news.cfm?newsid=17453183&BRD=1697&PAG=461&dept_id=44551&rft=6)

[[Return to top](#)]

## **General Sector**

Nothing to report.

[[Return to top](#)]

### **DHS Daily Open Source Infrastructure Report Contact Information**

[DHS Daily Open Source Infrastructure Reports](#) – The DHS Daily Open Source Infrastructure Report is a daily [Monday through Friday] summary of open-source published information concerning significant critical infrastructure issues. The DHS Daily Open Source Infrastructure Report is archived for ten days on the Department of Homeland Security Website:  
<http://www.dhs.gov/iaipdailyreport>

### **DHS Daily Open Source Infrastructure Report Contact Information**

Content and Suggestions:

Send mail to [dhsdailyadmin@mail.dhs.osis.gov](mailto:dhsdailyadmin@mail.dhs.osis.gov) or contact the DHS Daily Report Team at (703) 983-3644.

Subscription and Distribution Information:

Send mail to [dhsdailyadmin@mail.dhs.osis.gov](mailto:dhsdailyadmin@mail.dhs.osis.gov) or contact the DHS Daily Report Team at (703) 983-3644 for more information.

### **Contact DHS**

To report physical infrastructure incidents or to request information, please contact the National Infrastructure Coordinating Center at [nicc@dhs.gov](mailto:nicc@dhs.gov) or (202) 282-9201.

To report cyber infrastructure incidents or to request information, please contact US-CERT at [soc@us-cert.gov](mailto:soc@us-cert.gov) or visit their Web page at [www.us-cert.gov](http://www.us-cert.gov).

### **Department of Homeland Security Disclaimer**

The DHS Daily Open Source Infrastructure Report is a non-commercial publication intended to educate and inform



personnel engaged in infrastructure protection. Further reproduction or redistribution is subject to original copyright restrictions. DHS provides no warranty of ownership of the copyright, or accuracy with respect to the original source material.